What Is Claimed Is:

1.   A method for making available security functions for the
     transmission of data from and to a subscriber terminal
     unit of a mobile communications network,
     wherein a real-time analysis of the data flow (12) from
     and to the subscriber terminal unit (13) is carried out
     in a device (1) of a network node of the mobile
     communications network (10), data having contents
     specified previously by the subscriber or a network
     operator/provider being recognized and processed further.

2.   The method as recited in Claim 1,
     wherein the data traffic from and to specified senders
     and receivers is recognized and processed further.

3.   The method as recited in one of the preceding claims,
     wherein the recognized data are selected and/or isolated
     and/or deleted and/or made available to the subscriber or
     the network operator/provider separately for further
     processing.

4.   The method as recited in one of the preceding claims,
     wherein a filtering particularly of the IP/TCP-based data
     traffic is carried out.

5.   The method as recited in one of the preceding claims,
     wherein the arising data transfer volume is limited to a
     measure established by the subscriber or the network
     operator.

6.   The method as recited in one of the preceding claims,
     wherein the arising data transfer costs are limited to a
     measure established by the subscriber or the network
     operator.

7. The method as recited in one of the preceding claims, wherein the subscriber, network operator or provider is notified upon the recognition of certain data contents and/or senders.

8. A device for making available security functions for the transmission of data from and to a subscriber terminal unit of a mobile communications network, including a security and filtering device (1) having the following components:
    a filter component (2) for the real-time analysis of the data flow from and to the subscriber terminal unit;
    an authentication component (3) for authenticating the subscriber vis-à-vis the security and filtering device;
    an administrative component (4) as the interface to the subscriber; a database (5) for storing subscriber-specific and network operator-specific data as well as security and filtering functions.

9. The device as recited in Claim 9, wherein the security and filtering component (2) is established in one or more network nodes of the mobile communications network (10).

10. The device as recited in Claim 9 or 10, wherein for certain data contents, special filter components are established.